Discrete Mathematics 106/107 (1992) 311–316
North-Holland

Support weight distribution of linear codes

Torleiv Kløve
Department of Informatics, University of Bergen, Bergen, Norway

Received 4 November 1991
Revised 28 January 1992

Abstract

Kløve, T., Support weight distribution of linear codes, Discrete Mathematics 106/107 (1992) 311–316.

The main result of the paper is expressions for the support weight distributions of a linear code in terms of the support weight distributions of the dual code.

1. Introduction

Let C be an (n, k) code over GF(q). For any subcode D of C, we define the *support weight* of D to be the number of positions where not all the codewords of D are zero, and we denote it by $w_S(D)$. For $r \geq 0$ and $0 \leq i \leq n$, let $A_i^{(r)}$ be the number of r-dimensional subcodes of C of support weight i. The *rth support weight distribution* is the sequence

$$A_0^{(r)}, A_1^{(r)}, \ldots, A_n^{(r)},$$

and the *rth support weight distribution function* is the polynomial

$$A^{(r)}(Z) = A_0^{(r)} + A_1^{(r)}Z + \cdots + A_n^{(r)}Z^n.$$

For $0 \leq r \leq k$, the *the rth minimum support weight* is defined by

$$d_r(C) = \min\{w_S(D) \mid D \text{ is an } (n, r) \text{ subcode of } C\} = \min\{i \mid A_i^{(r)} \neq 0\}.$$

We note that $A^{(0)}(Z) = 1$. In [3, 6] we studied properties of codes which, by Lemma 1–4 below, are equivalent to support weight distributions; A_{ij} in [3, 6] is the same as $A_i^{(j)}$ in the notation above. Among other results in [3], we proved that $d_r(C) < d_{r+1}(C)$ for all r, a result rediscovered by Wei [8]; we also determined the support weight distribution of MDS codes. An application of the

Correspondence to: T. Kløve, Department of Informatics, University of Bergen, Thormøhlensgate 55, 5008 Bergen, Norway.

results in [6] was to determine the support weight distribution of the binary (23, 11) Golay code (without any computer search). Helleseth [2] determined the support weight distribution of some other classes of codes.

Wei [8] studied the minimum support weights (which he called generalized Hamming weights) in his analysis of the wire-tap channel of type II. His paper has sparked renewed interest in the subject. Further recent papers on the generalized Hamming weights (or minimum support weights) of binary codes are [1, 4]. Kasami et al. [5] used Wei's results in their analysis of the state complexity of the trellis diagrams of some binary codes.

We note that if $\bar{x} \in \mathrm{GF}(q)^n$, then

$$w_H(\bar{x}) = w_S(\{\bar{x}\}) = w_S(\{\lambda\bar{x} \mid \lambda \in \mathrm{GF}(q)\}).$$

Hence,

$$A^{(0)}(Z) + (q-1)A^{(1)}(Z) = A(Z),$$

the Hamming weight distribution function of C, and

$$d_1(C) = d_{min}(C).$$

Let $B^{(r)}(Z)$ be the rth support weight distribution function of the dual code $C^\perp$. We have

$$B^{(0)}(Z) = 1 = A^{(0)}(Z),$$

and, by MacWilliams' identity,

$$1 + (q-1)B^{(1)}(Z) = q^{-k}(1+(q-1)Z)^n\left\{1 + (q-1)A^{(1)}\left(\frac{1-Z}{1+(q-1)Z}\right)\right\}.$$

It is natural to ask if there are similar relations between the polynomials $B^{(r)}(Z)$ and $A^{(r)}(Z)$ for $r > 1$. The goal of this paper is to give such relations. Related results were given in [6].

2. Relations between the support weight distributions of a code and its dual

Let G be a generator matrix for C, and for any $\bar{x} \in \mathrm{GF}(q)^k$, let $\mu(\bar{x})$, the *multiplicity* of $\bar{x}$, be the number of occurrences of $\bar{x}$ as a column in G. Then $w_S(C) = n - \mu(\bar{0})$. Let

$$\mu(U) = \sum_{\bar{x} \in U} \mu(\bar{x}) \quad \text{for any } U \subseteq \mathrm{GF}(q)^k.$$

First we will give an alternative expression for $w_S(D)$, a similar result was given in [4].

If M is an $r \times k$ matrix of rank r, then MG generates an (n, r) subcode D of C, and any (n, r) subcode is obtained in this way. Let U_D be the space orthogonal to

the column space of M. Then

$$w_S(D) = n - \sum_{M\bar{x}=\bar{0}} \mu(\bar{x}) = n - \sum_{\bar{x}\in U_D} \mu(\bar{x}) = n - \mu(U_D).$$

This proves the following lemma.

Lemma 1. *Let D be a subcode of C. Then $w_S(D) = n - \mu(U_D)$.*

Let $F_l = \{U \mid U \text{ is a subspace of } \mathrm{GF}(q)^k \text{ of dimension } l\}$.

Lemma 2. *For any r where $0 \leq r \leq k$, $D \mapsto U_D$ is a bijection between the set of r-dimensional subspaces of C and the set F_{k-r}.*

In the sequel, we will use the following further notations:

$$[a]_b = \prod_{i=0}^{b-1} (q^a - q^i),$$

$$\langle a \rangle = [a]_a = \prod_{i=0}^{a-1} (q^a - q^i),$$

$$\begin{bmatrix} a \\ b \end{bmatrix} = \frac{[a]_b}{\langle b \rangle} \quad \text{(Gaussian binomial coefficient)}.$$

The number of b-dimensional subspaces of an a-dimensional vector space over $\mathrm{GF}(q)$ is given by the Gaussian binomial coefficient. Also, we note that

$$[a]_b = \frac{\langle a \rangle}{q^{b(a-b)}\langle a-b \rangle}.$$

Let $C^{(m)}$ be the code generated by G over $\mathrm{GF}(q^m)$.

In [7] we proved the following lemma (in a different notation). An equivalent result was given in [3]. For completeness we include the short proof.

Lemma 3. *The Hamming weight distribution function for $C^{(m)}$ is*

$$A_m(Z) = \sum_{r=0}^{k} [m]_r \sum_{U\in F_{k-r}} Z^{n-\mu(U)}.$$

Proof. Let

$$\hat{U} = \{\bar{y} \in \mathrm{GF}(q^m)^k \mid \bar{y} \cdot \bar{x} = 0 \quad \text{for } \bar{x} \in \mathrm{GF}(q)^k \text{ if and only if } \bar{x} \in U\}.$$

We note that if $\bar{y} \in \hat{U}$, then

$$w(\bar{y}G) = \sum_{\bar{x}\in \mathrm{GF}(q)^k} \mu(\bar{x}) w(\bar{y} \cdot \bar{x}) = \sum_{\bar{x}\in \mathrm{GF}(q)^k - U} \mu(\bar{x}) = n - \mu(U).$$

We further note that if $U \in F_r$, then

$$\sum_{\bar{y} \in \hat{U}} 1 = [m]_{k-r}.$$

Since $\{\hat{U} \mid U \text{ is a subspace of } \mathrm{GF}(q)^k\}$ is a partition of $\mathrm{GF}(q^m)^k$ we get

$$A_m(Z) = \sum_{r=0}^{k} \sum_{U \in F_r} \sum_{\bar{y} \in \hat{U}} Z^{w(\bar{y}G)} = \sum_{r=0}^{k} \sum_{U \in F_r} \sum_{\bar{y} \in \hat{U}} Z^{n-\mu(U)}$$

$$= \sum_{r=0}^{k} [m]_{k-r} \sum_{U \in F_r} Z^{n-\mu(U)} = \sum_{r=0}^{k} [m]_r \sum_{U \in F_{k-r}} Z^{n-\mu(U)}. \qquad \square$$

Lemma 4. *The Hamming weight distribution function $A_m(Z)$ of $C^{(m)}$ is*

$$A_m(Z) = \sum_{r=0}^{m} [m]_r A^{(r)}(Z).$$

Proof. Combining Lemmata 1–3 we get

$$A_m(Z) = \sum_{r=0}^{k} [m]_r A^{(r)}(Z).$$

Since $[m]_r = 0$ for $r > m$ and $A^{(r)}(Z) = 0$ for $r > k$, the lemma follows. $\square$

Since $(C^{(m)})^{\perp}$ is generated by the parity check matrix of C, the Hamming weight distribution of this code is

$$B_m(Z) = \sum_{r=0}^{m} [m]_l B^{(r)}(Z).$$

Hence, MacWilliams' identity for $C^{(m)}$ gives the following theorem.

Theorem 1. *For all $m \geq 0$ we have*

$$\sum_{r=0}^{m} [m]_r B^{(r)}(Z) = q^{-mk}\{1 + (q^m - 1)Z\}^n \left\{ \sum_{r=0}^{m} [m]_r A^{(r)}\left(\frac{1-Z}{1+(q^m-1)Z}\right)\right\}.$$

From Theorem 1 we can also get an explicit expression for $B^{(r)}(Z)$ in terms of the A's.

Theorem 2. *For all $r \geq 0$ we have*

$$B^{(r)}(Z) = \sum_{j=0}^{r} \sum_{l=0}^{j} (-1)^{r-j} \frac{q^{((r-j)(r-j-1)/2)-j(r-j)-l(j-l)-jk}}{\langle r-j\rangle \langle j-l\rangle}$$

$$\times \{1 + (q^j - 1)Z\}^n A^{(l)}\left(\frac{1-Z}{1+(q^j-1)Z}\right).$$

Proof. For convenience, we let

$$\alpha_{jl} = q^{-jk}\{1 + (q^j - 1)Z\}^n A^{(l)}\left(\frac{1-Z}{1+(q^j-1)Z}\right).$$

Define β_r by

$$\beta_r = \sum_{j=0}^{r}\sum_{l=0}^{j}(-1)^{r-j}\frac{q^{((r-j)(r-j-1)/2)-j(r-j)-l(j-l)}}{\langle r-j\rangle\langle j-l\rangle}\alpha_{jl}.$$

Then we have

$$\begin{aligned}
\sum_{r=0}^{m}[m]_r\beta_r &= \sum_{r=0}^{m}\frac{\langle m\rangle}{q^{r(m-r)}\langle m-r\rangle} \\
&\quad\times\sum_{j=0}^{r}\sum_{l=0}^{j}(-1)^{r-j}\frac{q^{((r-j)(r-j-1)/2)-j(r-j)-l(j-l)}}{\langle r-j\rangle\langle j-l\rangle}\alpha_{jl} \\
&= \sum_{j=0}^{m}\sum_{l=0}^{j}\alpha_{jl}\frac{q^{-j(m-j)-l(j-l)}\langle m\rangle}{\langle m-j\rangle\langle j-l\rangle} \\
&\quad\times\sum_{r=j}^{m}(-1)^{r-j}\frac{q^{((r-j)(r-j-1)/2)-(m-r)(r-j)}\langle m-j\rangle}{\langle m-r\rangle\langle r-j\rangle} \\
&= \sum_{j=0}^{m}\sum_{l=0}^{j}\alpha_{jl}\frac{q^{-j(m-j)-l(j-l)}\langle m\rangle}{\langle m-j\rangle\langle j-l\rangle} \\
&\quad\times\sum_{t=0}^{m-j}(-1)^t q^{t(t-1)/2}\begin{bmatrix} m-j \\ t\end{bmatrix} \\
&= \sum_{l=0}^{m}\alpha_{ml}\frac{q^{-l(m-l)}\langle m\rangle}{\langle m-l\rangle} = \sum_{l=0}^{m}\alpha_{ml}[m]_l
\end{aligned}$$

since (see e.g. [6, Lemma A.1])

$$\sum_{t=0}^{u}(-1)^t q^{t(t-1)/2}\begin{bmatrix} u \\ t\end{bmatrix} = \begin{cases}1 & \text{if } u = 0,\\ 0 & \text{if } u > 0.\end{cases}$$

We can now show by induction that $B^{(r)}(Z) = \beta_r$. First,

$$B^{(0)}(Z) = 1 = \beta_0.$$

Next, let $m > 0$ and suppose that $B^{(r)}(Z) = \beta_r$ for $r < m$. Then, by the result just proved above, Theorem 1, and the induction hypothesis,

$$\begin{aligned}
\langle m\rangle B^{(m)}(Z) &= \sum_{l=0}^{m}[m]_l\alpha_{ml} - \sum_{r=0}^{m-1}[m]_r B^{(r)}(Z) \\
&= \sum_{l=0}^{m}[m]_l\alpha_{ml} - \sum_{r=0}^{m-1}[m]_r\beta_r = \langle m\rangle\beta_m. \qquad \square
\end{aligned}$$

As a simple application of Theorem 2, we determine the support weight distributions of the Hamming codes. Let

$$n = (q^k - 1)/(q - 1),$$

and let G be a $k \times n$ matrix over GF(q) containing no zero columns, and no two columns where one is a multiple of the other; that is, G contains as columns exactly one multiple of each nonzero vector in GF$(q)^k$. Let C be the (n, k) code generated by G. Then $C^\perp$ is an $(n, n-k)$ Hamming code. If D is a subcode of C of dimension r, then, by Lemma 1,

$$w_S(D) = \frac{q^k - 1}{q - 1} - \frac{q^{k-r} - 1}{q - 1} = \frac{q^k - q^{k-r}}{q - 1}.$$

Hence

$$A^{(r)}(Z) = \begin{bmatrix} k \\ r \end{bmatrix} Z^{(q^k - q^{k-r})/(q-1)}.$$

By Theorem 2 we get

$$B^{(r)}(Z) = \sum_{j=0}^{r} \sum_{l=0}^{j} (-1)^{r-j} \frac{q^{((r-j)(r-j-1)/2) - j(r-j) - l(j-l) - jk}}{\langle r-j \rangle \langle j-l \rangle} \begin{bmatrix} k \\ l \end{bmatrix} \times (1 - Z)^{(q^k - q^{k-l})/(q-1)} \{1 + (q^j - 1)Z\}^{(q^{k-l} - 1)/(q-1)}.$$

References

[1] G.L. Feng, K.K. Tzeng and V.K. Wei, On the generalized Hamming weights of several classes of cyclic codes, submitted for publication, 1990.

[2] T. Helleseth, The weight enumerator polynomials of some classes of codes with composite parity-check polynomials, Discrete Math. 20 (1977) 21–31.

[3] T. Helleseth, T. Kløve and J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/N)$, Discrete Math. 18 (1977) 179–211.

[4] T. Helleseth, T. Kløve and Ø. Ytrehus, Generalized Hamming weights of linear codes, IEEE Trans. Inform. Theory 38 (1992); presented in part at the 4th Internat. Colloq. on Coding Theory, Dilijan, Armenia, 1991.

[5] T. Kasami, T. Takata, T. Fujiwara and S. Lin, On the state complexity of trellis diagrams for Reed–Muller codes and their supercodes, presented at the 4th Internat. Colloq. on Coding Theory, Dilijan, Armenia 1991.

[6] T. Kløve, The weight distribution of linear codes over GF(q^l) having generator matrix over GF(q), Discrete Math. 23 (1978) 159–168.

[7] T. Kløve, Optimal codes for error detection, IEEE Trans. Inform. Theory 38 (1992) 479–489.

[8] V.K. Wie, Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412–1418.